UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

JULIA ROSSI, DELILAH PARKER, and KELVIN HOLMES, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CLAIRE'S STORES, INC.; CLAIRE'S BOUTIQUES, INC.; and CBI DISTRIBUTING CORP.,

Defendants.

Case No. 1:20-cv-05090

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Hon. Andrea R. Wood, presiding

Plaintiffs Julia Rossi, Delilah Parker and Kelvin Holmes (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege upon personal knowledge as to their own actions, investigation of counsel, and on information and belief as follows:

SUMMARY OF THE CASE

1. This class action arises as a result of Claire's Stores, Inc., Claire's Boutiques, Inc., and CBI Distributing Corp. (collectively, "Claire's" or "Defendants"), worldwide jewelry and fashion accessory retailers, permitting an unauthorized intrusion of their e-commerce websites that compromised the personal and financial information of their customers.

2. Defendants specialize in selling low-priced jewelry and accessories to young women and girls. Defendants operate internationally through their retail stores under two brand names, Claire's® and Icing®. Defendants also sell their products online through their popular

websites. For online sales, Defendants use e-commerce platforms supported by salesforce.com, inc. to take customers' personal and payment information.

3. On or about June 12, 2020, Defendants first learned that they were experiencing a data breach that resulted in the unauthorized access, disclosure, acquisition, and/or use of unsecured personal and financial information from online customer purchases from at least April 7, 2020 through June 12, 2020 (the "Data Breach"). The compromised customer information included, without limitation, first and last names, addresses, email addresses, phone numbers, payment card numbers, payment card expiration dates, payment card verification codes, and account passwords, as well as gift card numbers and gift card PINs, if applicable (collectively, "Personal Information"). As a result of the Data Breach, the security and privacy of Plaintiffs' and Class Members' Personal Information was compromised.

4. Defendants had no idea the breach was happening. Defendants investigated their e-commerce website only after they were contacted by a third party on June 11, 2020, who determined that the e-commerce platforms on claires.com and icing.com had been hacked.[1] Defendants have indicated they discovered that the "added code was capable of obtaining information entered by customers during the checkout process and sending it out of the Claire's system."

[1] *See, e.g.,* Exhibit 1 (Defendants' Data Breach Notice Letter to Plaintiff Parker); *Claire's Notice of Data Breach to the Washington Attorney General*, July 8, 2020, archived by the Washington Attorney General, *available at*: https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/Claire%27sStoresInc.2020-07-08.pdf (Claire's Notice of Data Breach, addressed to affected customers, is included at pages 3-7).

5. After investigating the Data Breach, Defendants waited nearly one full month, at minimum, to provide notice to their affected customers, including Plaintiffs, via a data breach notification letter dated on or about July 7, 2020 (the "Notice Letter").

6. In addition to revealing the Personal Information compromised in the Data Breach, the Notice Letter characterizes the Data Breach as "computer code that had been added to our site by an unauthorized person" that "was capable of obtaining information entered by customers during the checkout process and sending that information out of our system." The Notice Letter further indicates that Defendants notified the recipients "because [they] placed an order during a time the added code was present."

7. Plaintiffs' and Class Members' unsecured Personal Information compromised in the Data Breach as a direct result of Defendants' acts and/or omissions included the types of personal and financial information that people consider extremely sensitive and private. This extremely sensitive data should have received the most rigorous protection available, but it did not.

8. Defendants were collecting and storing Plaintiffs' and Class Members' sensitive and confidential Personal Information, which they knew consumers consider to be extremely private and which is valuable to criminals and vulnerable to exfiltration. Defendants failed to take security precautions necessary to protect the Personal Information.

9. Because Defendants failed to take necessary security precautions, Plaintiffs' and Class Members' Personal Information was disclosed and exfiltrated by unauthorized persons, who now have been and will continue to be able to sell the compromised Personal Information for financial fraud and identity theft purposes.

PARTIES

10. Plaintiff Julia Rossi is a citizen of Pennsylvania residing in Dauphin County. Ms. Rossi purchased items from Defendants' website on or about May 30, 2020. She received a Notice Letter, dated July 7, 2020, on or about that date, which specifically identified her credit card as the payment card exposed by the Data Breach.

11. Plaintiff Delilah Parker is a citizen of Tennessee residing in Davidson County. Ms. Parker purchased items from Defendants' website on or about May 24, 2020. She received a Notice Letter, dated July 7, 2020, on or about that date, which specifically identified her debit card as the payment card exposed by the Data Breach.

12. Plaintiff Kelvin Holmes is a citizen of Georgia residing in Polk County. Mr. Holmes purchased items from Defendants' website on or about May 25, 2020. He received a Notice Letter, dated July 7, 2020, on or about that date, which specifically identified his debit card as the payment card exposed by the Data Breach.

13. Defendant Claire's Stores, Inc. is a Florida corporation with its principal place of business in Hoffman Estates, Illinois. As self-described on its website, Claire's Stores, Inc. is "one of the world's leading specialty retailers of fashionable jewelry and accessories."[2]

14. Defendant Claire's Boutiques, Inc. is a Michigan corporation with its principal place of business in Hoffman Estates, Illinois. Upon information and belief, Claire's Boutiques, Inc. is a wholly owned subsidiary of Claire's Stores, Inc. that operates Defendants' e-commerce websites. Prior to September 4, 2020, Claire's Boutiques, Inc. was a Colorado corporation.

---

[2] *See* https://www.clairestores.com/company-profile/company-overview.

15. Defendant CBI Distributing Corp. is a Delaware corporation with its principal place of business in Hoffman Estates, Illinois. Upon information and belief, CBI Distributing Corp. is a wholly owned subsidiary of Claire's Stores, Inc. and operates Defendants' e-commerce websites where the Data Breach occurred.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiffs are diverse from Defendants, as Defendants are not citizens of any of the states in which Plaintiffs reside.

17. This Court has personal jurisdiction over Defendants because Defendants have systematic and continuous contacts with Illinois through their websites and because their headquarters are located within this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendants reside within this District and substantial parts of the events giving rise to the claims alleged herein occurred within this District.

STATEMENT OF FACTS

A. Defendants' Data Breach and Subsequent Notice to Affected Customers

19. Defendants are large retail and online sellers of jewelry and other fashion accessories. Defendants operate in over 40 countries, with over 2,000 retail locations in North America and Europe and over 7,000 store locations in the rest of the world.[3]

20. Between 2014 and 2017, Defendants' net sales reportedly averaged nearly $1.4 billion annually. In 2019 alone, Defendants' global net sales for online purchases through their websites—claires.com and icing.com—reportedly were $12.9 million.

21. Defendants ensure their customers that they are concerned about Personal Information security: "We take data privacy very seriously and work super hard to protect your personal information."[4] *Super hard* is apparently not hard enough. Defendants also claim:

> SECURITY
> We believe in providing a safe and secure experience for all of our customers and the Site visitors. To that end we have implemented security measures to protect the information collected from you. All information you provide to us is stored on our secure servers and on the servers of cloud-based service providers. The computers and servers on which we store personal information are kept in a secure environment. **While we use encryption to protect sensitive information transmitted online, we also protect your information offline.** Payment transactions may be undertaken by third party service providers and will be encrypted using industry standard SSL technology. Where we have given you (or where you have chosen) a password which enables you to access your online account, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.
>
> We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it. Every employee accessing systems containing your personal information has a separate unique username and password. Access to your personal information is limited to those employees who require such access to perform their job duties. In addition,

---

[3] *Id.*
[4] Claire's Privacy Policy, dated May 15, 2018, available at: https://www.claires.com/us/privacypolicy.html.

> we train our employees about the importance of confidentiality and maintaining the privacy and security of your personal information. We commit to taking appropriate disciplinary measures to enforce our employees' privacy responsibilities [.] (emphasis added).[5]

22. Defendants do not claim that they abide by the PCI DSS (Payment Card Industry Data Security Standard) compliance, which is a requirement for businesses that store, process, or transmit payment card data.

23. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions. Businesses that fail to maintain PCI DSS compliance are subject to steep fines and penalties.

24. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[6]

25. To purchase items on Defendants' websites, customers can either create an account or check out as a guest. Either choice requires, at a minimum, that the customer enter the following Personal Information onto the website:

- Name;
- billing address;
- shipping address;
- email address;
- telephone number;

---

[5] *Id.*; *see also* Icing's Privacy Policy, which mirrors Claire's verbatim, available at: https://www.icing.com/us/privacy-policy.html.

[6] PCI Security Standards Council, available at: https://www.pcisecuritystandards.org/.

- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code or CVV code (card verification number)

26. When a customer purchases items on Defendants' websites, as a guest or through an account, they are not asked to acknowledge the "Privacy Policy," and they are not asked to read the "Terms of Use." Links to Claire's and Icing's "Privacy Policy" and "Terms of Use" are included on the extreme bottom right borders of the website pages in black, unremarkable font, with no indications of hyperlinks to the policies or terms. The "Privacy Policy" and "Terms of Use," however, do not appear at all on the mobile webpage unless the user clicks on the "About Us" link. Similarly, there are no links to the "Terms of Use" on the e-commerce platform where the purchase is finalized, only a terse statement in uniform font stating that the customer is "agreeing to our terms and conditions."

27. In or around June 2020, reports surfaced that Defendants had recently experienced a cyber intrusion on their e-commerce platform by hackers using Magecart tactics.[7] These hackers reportedly infiltrated Defendants' Salesforce Commerce Cloud environment for at least seven weeks.[8]

28. Upon information and belief, Defendants did not issue a press release regarding the Data Breach but confirmed the Data Breach through press inquiries.

---

[7] *See, e.g.*, Mathew J. Schwartz, *Claire's: Magecart E-Commerce Hackers Stole Card Data*, BANKINFO SECURITY, June 15, 2020, https://www.bankinfosecurity.com/claires-says-magecart-e-commerce-hackers-stole-card-data-a-14436.

[8] *Id.*

29. The Data Breach resulted in the unauthorized access, disclosure, acquisition, and/or use of the Personal Information of Plaintiffs and Class Members. In particular, the hackers added computer code to Defendants' e-commerce websites that obtained full payment card details and other Personal Information entered by customers during the checkout process and exfiltrated that information out of Defendants' systems and into the hands of unauthorized persons.

30. As a result of the Data Breach, the security and privacy of Plaintiffs' and Class Members' Personal Information, including sensitive financial information, was compromised.

31. Although Defendants knew of the Data Breach no later than June 12, 2020 (and likely earlier), Defendants took no steps to notify customers whose information was compromised until on or about July 7, 2020, when Defendants began mailing Notice Letters to the affected individuals directly.

32. To date, Defendants' websites do not contain any information or notice regarding the Data Breach. Defendants' online "Press Room" also contains no reference to the Data Breach.[9]

33. The Notice Letter indicated, in part, the following:

> Claire's and Icing are writing to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.
>
> **What Happened?**
>
> We recently began an investigation of our e-commerce websites, and on June 12, 2020 we identified and removed computer code that had been added to our site by an unauthorized person. The added code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. A security firm was engaged and we identified the specific transactions involved. We also reinforced the security of our site. Purchases made in our retail store locations were not involved.

[9] *See* https://www.clairestores.com/financial-press-release.

> Findings from the investigation show the code was first added on April 7, 2020. There were several times from April 7 to June 12 when the added code was not present because of new code deployments. We are notifying you because you placed an order during a time the added code was present.
>
> **What Information Was Involved?**
>
> The information entered during the checkout process that could have been copied includes:
>
> - **Contact information** – first and last name, address, email address (only if you chose to edit your email on the checkout page), and phone number.
> - **Payment card information** – payment card number, expiration date, and card verification code for the payment card ending in [XXXX]. If you made more than one purchase between April 7 and June 12 and used more than one card, you can identify the other cards involved by looking at your email receipt or by calling us at the number below.
> - **Other information** – if you paid with a gift card or created a Claire's account during the checkout process, the added code could have copied the gift card number and PIN or the account password (but not the email address).

34. Further, Defendants' Notice Letter acknowledged the very real threat that the incident would result in identity theft, fraud, and other similar risks by further encouraging recipients—Plaintiffs and Class Members—to "closely review your payment card account statements for any unauthorized charges." The Notice Letter also instructed victims to "immediately report any unauthorized charges to the bank that issued your card . . . ."

35. Defendants also acknowledged their failure to safeguard customers' Personal Information, concluding the Notice Letter with an apology: "We regret that this occurred and apologize for any inconvenience."

36. Defendants' own statements confirm that Plaintiffs and Class Members are subject to continued, future risk of identity theft, fraudulent charges, and other damages. Further, Defendants offered only one year of identity theft insurance, a level and duration of protection

both woefully inadequate to address the risk of identity theft and fraud Defendants created by negligently allowing the Data Breach to occur.

37. By acknowledging the exfiltration of Personal Information in the Notice Letter, Defendants reasonably believe and concede that Plaintiffs' and Class Members' unencrypted Personal Information was acquired and viewed by unauthorized persons as a result of the Data Breach.

38. Further, Defendants reasonably believe and concede security, confidentiality, and/or integrity of Plaintiffs' and Class Members' unencrypted Personal Information was compromised by Defendants as a result of the Data Breach.

39. It is reasonable to infer and should be rebuttably presumed that Plaintiffs' and Class Members' unencrypted Personal Information that was acquired by unauthorized persons as a result of the Data Breach and was viewed by unauthorized persons.

40. After receiving the Notice Letter, it is reasonable for recipients—Plaintiffs and Class Members—to believe that future harm (including identity theft) is real and imminent, and for them to take steps to mitigate that risk of future harm.

B. Defendants Had an Obligation to Protect Personal Information Under the Applicable Law and Standard of Care.

41. Defendants had obligations created and imposed by state laws, and based on industry standards, to keep the compromised Personal Information confidential and to protect it from unauthorized disclosure. Plaintiffs and Class Members provided their Personal Information to Defendants with the common-sense understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized disclosure.

42. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches—particularly those in the retail industry—which were widely known to the public and to anyone in Defendants' industry.

43. Defendants' security failures demonstrate that they failed to honor their duties and promises by not: (1) maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks; (2) adequately protecting Plaintiffs' and Class Members' Personal Information; (3) ensuring the confidentiality and integrity of the electronic Personal Information of customers; (4) implementing technical policies and procedures for electronic information systems that maintain customers' Personal Information to allow access only to those persons or software programs that have been granted access rights; (5) implementing policies and procedures to prevent, detect, contain, and correct security violations; (6) implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports; (7) protecting against any reasonably anticipated threats or hazards to the security or integrity of customers' Personal Information; (8) and training all members of their workforce effectively on the policies and procedures with respect to protecting customers' Personal Information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of customers' Personal Information.

44. As described before, Defendants also are required (by various other states' laws and regulations) to protect Plaintiffs' and Class Members' Personal Information, and, further, to handle any breach of the same in accordance with applicable breach notification statutes.

45. In addition to their obligations under state laws, Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting the Personal

Information in their possession from being compromised, lost, stolen, disclosed, accessed, viewed, and/or misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, consistent with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of Plaintiffs and Class Members.

46. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to design, maintain, and test their computer systems to ensure that the Personal Information in Defendants' possession was adequately secured and protected.

47. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to create and implement reasonable data security practices and procedures to protect the Personal Information in their possession, including adequately training their employees and others who accessed Personal Information within their computer systems on how to adequately protect Personal Information.

48. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to implement processes that would detect a breach or leak on their data security systems in a timely manner.

49. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to adequately train and supervise their employees to detect a breach or leak on their data security systems in a timely manner.

50. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to act upon data security warnings and alerts in a timely fashion.

51. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to disclose if their computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' Personal Information from exfiltration or leaks because such an inadequacy would be a material fact in the decision to entrust Personal Information to Defendants.

52. Defendants owed a duty to Plaintiffs and Class Members whose Personal Information was entrusted to Defendants, to disclose in a timely and accurate manner when data breaches or leaks occurred.

53. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

C. It is Well Established That Data Breaches Lead to Identity Theft and Other Harms.

54. Plaintiffs and Class Members have been injured by the release, disclosure, and exfiltration of their Personal Information in the Data Breach.

55. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[10] Cyber criminals can leverage Plaintiffs' and Class Members' Personal Information that was released, disclosed, and exfiltrated in the Data Breach to commit thousands of crimes, including: opening new financial accounts and taking out loans in Plaintiffs' and Class Members' names; using Plaintiffs' and Class Members' Personal Information to file fraudulent tax returns and obtain government benefits; obtaining driver's licenses in Plaintiffs' and Class Members' names but with another person's photograph; giving false information to police during an arrest;

---

[10] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

and, of course, using Plaintiffs' and Class Members' payment card information to make any number of fraudulent purchases. Even worse, Plaintiffs and Class Members could be arrested for crimes identity thieves have committed.[11]

56. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised criminals often trade the information on the cyber black-market for years.

57. This is not just speculative. As the FTC has reported, if hackers get access to Personal Information, they **will** use it.[12]

58. Further, even if identity thieves obtain only some Personal Information, that information can be successfully used when aggregated or combined with other sensitive identifying information to form a complete "profile" of the victim, ripe for identity theft. If cyber criminals manage to acquire Personal Information, including financial information such as credit and debit card numbers, along with other sensitive information, such as Social Security numbers, driver's licenses, or passport numbers, there is no limit to the amount of fraud to which Defendants have exposed Plaintiffs and Class Members.

59. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[13] As the

---

[11] *Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

[12] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N, May 24, 2017, https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[13] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), U.S. GOV'T ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/new.items/d07737.pdf.

GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

60. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[14]

61. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit.[15] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

62. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, ***stolen data may be held for up to a year or more before being used to commit identity theft***. Further, once stolen data have been sold or posted on the Web, ***fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

63. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers and other Personal Information directly on various Internet websites making the information publicly available.

---

[14] *Id.* at 2, 9.
[15] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, Sept. 2013, https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[16] *Id*. at 29 (emphases added).

64. To date, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than offering them one year of identity theft insurance and telling them to simply "review your payment card account statements regularly for any unauthorized charges" and "report any unauthorized charges to your bank." None of these recommendations or offers, however, require Defendants to expend any material effort, or take reasonable measures, to protect Plaintiffs' and Class Members' Personal Information.

65. The Personal Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

66. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

---

[17] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[18] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[19] *In the Da*rk, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

67. Defendants' retail locations were closed and customers could only get Defendants' products from Defendants' websites. Defendants therefore were, or should have been, fully aware of the significant volume of daily credit and debit card transactions taking place on their websites and therefore the significant number of individuals who would be harmed by a breach of Defendants' systems.

68. Defendants' failure to adequately protect Plaintiffs' and Class Members' Personal Information has resulted in Plaintiffs and Class Members having to undertake protective and mitigating measures, which require extensive amounts of time, calls, and, for many of the more adequate credit and fraud protection services, payment of money—while Defendants sit by and do nothing to assist those affected by the Data Breach. Instead, as Defendants' Notice Letter indicates, they are placing the burden on Plaintiffs and Class Members to discover and rectify fraudulent activity and identity theft.

69. Defendants' offer of twelve months of "Internet surveillance" and identity theft insurance is woefully inadequate. While some harm has already begun to occur, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal Information); it does not prevent identity theft.[20]

[20] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

70. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance accounts for unauthorized activity for years to come.

71. Plaintiffs and the Class Members have suffered, continue to suffer and/or will suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper release and disclosure of their Personal Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Deprivation of the value of Plaintiffs' and Class Members' Personal Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items, which a reduced credit score adversely affects.

72. Moreover, Plaintiffs and Class Members have an interest in ensuring that their information, which remains in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards.

D. Plaintiffs' Experiences

Plaintiff Julia Rossi

73. Defendants received and collected Plaintiff Julia Rossi's Personal Information when she purchased merchandise from Defendants' websites, which Defendants maintained in their computer systems. Defendants then disclosed Ms. Rossi's Personal Information to unauthorized third parties as a result of the Data Breach.

74. In July 2020, Ms. Rossi received a Notice Letter dated July 7, 2020 from Marie Hodge, Defendants' Executive Director of Communications and Operations, notifying Ms. Rossi of the Data Breach. The contents of the Notice Letter are the same as those previously alleged herein.

75. Since June 2020, Ms. Rossi has experienced a substantial increase in spam/phishing calls from persons apparently attempting to defraud her. In many instances, these fraudulent callers

leave threatening or otherwise deceptive voice messages in an attempt to obtain additional Personal Information from Ms. Rossi.

76. Prior to the Data Breach, Ms. Rossi was not regularly receiving spam/phishing calls. Since the Data Breach occurred, Ms. Rossi has been receiving these calls on a daily basis, often multiple calls per day.

77. Ms. Rossi now engages in daily monitoring of her financial accounts for fraudulent activity, including, without limitation, the account compromised in the Data Breach. She also has spent significant time reviewing her financial records for signs of fraudulent credit activity.

78. Since learning of the Data Breach, Ms. Rossi has spent several hours per day of her own time attempting to mitigate the risks of fraud and identity theft created by Defendants. Further, Ms. Rossi now spends significant time on a daily basis dealing with a high volume of phishing calls and voice messages.

79. Because Ms. Rossi received the Notice Letter from Defendants, it is and was reasonable for her to believe that future harm (including fraudulent charges and identity theft) is and was real and imminent, and to take steps to mitigate that risk of future harm.

80. Had Ms. Rossi known that Defendants were not maintaining customers' Personal Information with adequate security and that Defendants' systems were susceptible to data breaches, Ms. Rossi would not have provided her Personal Information to Defendants to purchase merchandise on Defendants' websites.

81. Ms. Rossi is not aware of any other data breaches that could have resulted in the theft of her debit card information. She is very careful about sharing her Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

82. Ms. Rossi stores any and all documents containing her Personal Information in a safe and secure digital location and destroys any documents she receives in the mail that contain any of her Personal Information or that may contain any information that could otherwise be used to compromise her payment card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

83. Ms. Rossi suffered actual injury by being forced to review phishing emails and in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which she would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' Personal Information from theft.

84. Ms. Rossi suffered actual injury in the form of damages to and diminution in the value of her Personal Information—a form of intangible property that Ms. Rossi entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

85. Further, a portion of the price Ms. Rossi paid for the merchandise she purchased on Defendants' websites, like all other revenue Defendants obtained from customers, was or should have been allocated by Defendants to adequately safeguard customers' Personal Information, but it was not. Thus, Ms. Rossi and Class Members overpaid for the online merchandise they purchased from Defendants and are entitled to restitution for that overpayment.

86. Ms. Rossi suffered lost money, time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of her privacy.

87. Ms. Rossi has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal Information being placed in the hands of criminals.

88. Ms. Rossi has become worried about this theft of her Personal Information and has a continuing interest in ensuring that Defendants protect and safeguard her Personal Information, which remains in their possession, from future breaches.

Plaintiff Delilah Parker

89. Plaintiff Delilah Parker accessed Claire's website from her home on or about May 24, 2020, via her smartphone and purchased items for a total of $29.01. Claire's shipped the items to her on or about May 28, 2020.

90. Ms. Parker made this purchase through the claires.com website as a guest. She entered her Personal Information into Defendants' e-commerce payment platform, including her full name, billing and shipping addresses, debit card type and full number, CVV code, debit card expiration date and email address.

91. During this transaction, Defendants did not ask or direct Ms. Parker to "agree" to or even review Claire's "Privacy Policy," nor did they instruct her to read the "Terms of Use."

92. Ms. Parker received the Notice of Data Breach, dated July 7, 2020, on or about that date.

93. Beginning on or about August 17, 2020, unknown third parties used Ms. Parker's debit card – the same payment card she used on Defendants' hacked e-commerce platform – to make unauthorized purchases in Washington, Georgia, and California via the internet. The purchases total over $700 so far. The money was withdrawn from Ms. Parker's checking account

on or about August 18, 2020, and although her bank confirmed the charges were unauthorized, the bank did not fully reimburse her for the losses until August 24, 2020.

94. As a result of the Data Breach notice and the theft of her funds, Ms. Parker spent time dealing with the consequences of the breach, which included time spent confirming that she made a purchase using her debit card during the relevant period, reviewing the account compromised by the breach, contacting her bank, self-monitoring her accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Claire's.

95. Although Ms. Parker enrolled in the credit monitoring service offered by Claire's in July 2020, the monitoring did not help prevent or notify her about the unauthorized use of her debit card in August 2020. In the Notice of Data Breach, Claire's did not advise affected customers to change their payment card account numbers. Rather, Claire's stated that they already "notified the payment cards network so that they can inform the banks that issued the cards," and encouraged victims only "to closely review your payment card account statements for any unauthorized charges."[21]

96. Ms. Parker is not aware of any other data breaches that could have resulted in the theft of her debit card information. She is very careful about sharing her Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

97. Ms. Parker stores any and all documents containing her Personal Information in a safe and secure digital location and destroys any documents she receives in the mail that contain

[21] *See* Exhibit 1.

any of her Personal Information or that may contain any information that could otherwise be used to compromise her payment card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

98. Ms. Parker suffered actual injury and damages in losing over $700 from her bank account and in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which she would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' Personal Information from theft.

99. Ms. Parker suffered actual injury in the form of damages to and diminution in the value of her Personal Information—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

100. Further, a portion of the price Ms. Parker paid for the merchandise she purchased on Defendants' websites, like all other revenue Defendants obtained from customers, was or should have been allocated by Defendants to adequately safeguard customers' Personal Information, but it was not. Thus, Ms. Parker and Class Members overpaid for the online merchandise they purchased from Defendants and are entitled to restitution for that overpayment.

101. Ms. Parker suffered lost money, time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of her privacy.

102. Ms. Parker has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal Information being placed in the hands of criminals.

103. Ms. Parker has become worried about this theft of her Personal Information and has a continuing interest in ensuring that her Personal Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

Plaintiff Kelvin Holmes

104. Plaintiff Kelvin Holmes accessed Claire's website from his home on or about May 25, 2020 via his smartphone and purchased items for a total of $27.65. Claire's shipped the items to him on or about May 25, 2020.

105. Mr. Holmes made this purchase through the claires.com website as a guest. He entered his Personal Information into Defendants' e-commerce payment platform, including his full name, billing and shipping addresses, telephone number, debit card type and full number, CVV code, debit card expiration date and email address.

106. During this transaction, Defendants did not ask Mr. Holmes to "agree" to or even review Claire's "Privacy Policy," nor did they instruct him to read the "Terms of Use."

107. Mr. Holmes received the Notice of Data Breach, dated July 7, 2020, on or about that date.

108. Subsequent to the Data Breach, Mr. Holmes began receiving a marked increase in the number of suspicious phishing emails containing fraudulent links. Reviewing these emails to determine their legitimacy has taken time that Mr. Holmes otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

109. As a result of receiving the Data Breach notice and the subsequent suspicious emails, Mr. Holmes has spent time dealing with the consequences of the breach, including confirming he made a purchase using his debit card during the relevant period, reviewing the account compromised by the breach, contacting his bank, self-monitoring his accounts, exploring

credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Claire's.

110. Mr. Holmes is not aware of any other data breaches that could have resulted in the theft of his debit card information. He is very careful about sharing his Personal Information, and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source.

111. Mr. Holmes stores any and all documents containing his Personal Information in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his Personal Information or that may contain any information that could otherwise be used to compromise his payment card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts, and periodically changes his passwords for added security.

112. Mr. Holmes suffered actual injury being forced to review phishing emails and in paying money to, and purchasing products from, Defendants' website during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' Personal Information from theft.

113. Mr. Holmes suffered actual injury in the form of damages to and diminution in the value of his Personal Information—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

114. Further, a portion of the price Mr. Holmes paid for the merchandise he purchased on Defendants' websites, like all other revenue Defendants obtained from customers, was or

should have been allocated by Defendants to adequately safeguard customers' Personal Information, but it was not. Thus, Mr. Holmes and Class Members overpaid for the online merchandise they purchased from Defendants and should be entitled to restitution for that overpayment.

115. Mr. Holmes also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

116. Mr. Holmes has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of criminals.

117. Mr. Holmes has become worried about this theft of his Personal Information and has a continuing interest in ensuring that Defendants protect and safeguard his Personal Information, which remains in their possession, from future breaches.

CLASS ALLEGATIONS

118. Plaintiffs bring this class action pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all others similarly situated.

119. Plaintiffs seek certification of a Nationwide Class, a Pennsylvania Subclass, a Tennessee Subclass, and a Georgia Subclass (collectively, the "Class") defined as follows:

> Nationwide Class: All persons in the United States whose Personal Information was compromised as a result of the Data Breach Defendants disclosed on or about July 7, 2020.
>
> Pennsylvania Subclass: All persons residing in the Commonwealth of Pennsylvania whose Personal Information was compromised as a result of the Data Breach Defendants disclosed on or about July 7, 2020.
>
> Tennessee Subclass: All persons residing in Tennessee whose Personal Information was compromised as a result of the Data Breach Defendants disclosed on or about July 7, 2020.

Georgia Subclass: All persons residing in Georgia whose Personal Information was compromised as a result of the Data Breach Defendants disclosed on or about July 7, 2020.

120. Specifically excluded from the Class are Defendants and any entities in which Defendants have a controlling interest, Defendants' agents and employees, the judge to whom this action is assigned, members of the judge's staff, and the judge's immediate family.

121. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

122. **Numerosity:** Plaintiffs do not know the exact number of Class Members but are informed and believe the Class comprises many thousands of individuals throughout the United States. As such, Class Members are so numerous that joinder of all Members is impracticable.

123. **Commonality and Predominance:** Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiffs' and Class Members' Personal Information;

c. Whether Defendants failed to protect Plaintiffs' and Class Members' Personal Information properly and/or as promised;

d. Whether Defendants' computer system and data security practices used to protect Plaintiffs' and the Class Members' Personal Information violated applicable state law, and/or Defendants' duties to safeguard the information;

e. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and Class Members' Personal Information;

f. Whether Defendants violated the consumer protection statutes and/or data breach notification statutes applicable to Plaintiffs and Class Members;

g. Whether Defendants failed to notify Plaintiffs and Class Members about the Data Breach as soon as practicable and without delay after the Data Breach was discovered;

h. Whether Defendants acted negligently in failing to safeguard Plaintiffs' and Class Members' Personal Information;

i. Whether Defendants breached their express or implied contractual obligations to protect the confidentiality of Plaintiffs' and the Class Members' Personal Information, and to maintain reasonable data security measures;

j. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

l. What equitable relief is appropriate to redress Defendants' wrongful conduct; and

m. What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members.

124. **Typicality:** Plaintiffs' claims are typical of the claims of the other Class Members. Defendants' uniform misconduct injured Plaintiffs and Class Members and Plaintiffs' and Class Members' legal claims all arise from Defendants' core practices.

125. **Adequacy:** Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and there are no defenses

unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to those of the other members of the Class.

126. **Superiority:** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class Member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring each affected Class Member to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. Plaintiffs anticipate no unusual difficulties in managing this class action.

COUNT I
Negligence

127. Plaintiffs incorporate herein every previously alleged factual allegation.

128. Plaintiffs bring this count on behalf of the National Class or, in the alternative, the Pennsylvania Subclass, Tennessee Subclass, and/or Georgia Subclass.

129. Defendants solicited, collected, and stored Plaintiffs' and Class Members' Personal Information.

130. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class Members' Personal Information and the importance of adequate security.

131. Defendants were well aware of the fact that hackers routinely attempt to access Personal Information without authorization. Defendants also knew about numerous, well-

publicized data breaches wherein hackers stole the Personal Information from other retailers who held or stored such information.

132. Defendants owed duties of care to Plaintiffs and Class Members who entrusted their Personal Information with Defendants.

133. Defendants owed a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and Class Members when obtaining, storing, using, and managing their Personal Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and Class Members of any breach in a timely manner so that they could take appropriate action to minimize or avoid losses.

134. This duty extends to protecting others from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard Personal Information.

135. Plaintiffs and Class Members were the intended beneficiaries of Defendants' duty to safeguard their Personal Information, creating a special relationship between them and Defendants. Only Defendants were in a position to ensure that their systems were sufficient to protect Plaintiffs' and Class Members' Personal Information entrusted to Defendants.

136. Defendants also were subject to an independent duty to safeguard Plaintiffs' and Class Members' Personal Information that was untethered to any contract between Defendants and Plaintiffs and Class Members.

137. In addition to the general duties above, Defendants' duties specifically included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Personal Information in their possession;

b. To protect Personal Information in their possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store Personal Information;

d. To implement processes to quickly detect a data breach, security incident, or intrusion; and

e. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

138. It was foreseeable that injury to Plaintiffs and Class Members would result from Defendants' violation of these duties in mishandling Plaintiffs' and Class Members' Personal Information.

139. Because Defendants knew that a security incident, breach, or intrusion upon their systems would potentially damage hundreds of thousands of individuals, including Plaintiffs and Class Members, Defendants had a duty to adequately protect their Personal Information.

140. Defendants knew, or should have known, that their security practices and computer systems did not adequately safeguard Plaintiffs' and Class Members' Personal Information.

141. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and security practices to safeguard Plaintiffs' and Class Members' Personal Information.

142. Defendants breached their duties of care by failing to provide prompt notice of the Data Breach to Plaintiffs and Class Members.

143. Defendants acted with reckless disregard for the security of Plaintiffs' and Class Members' Personal Information because Defendants knew or should have known that their computer systems and data security practices were not adequate to safeguard the Personal Information that they collected and stored.

144. Defendants acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate notice of the Data Breach so they could take measures to protect themselves from damages caused by the fraudulent use of Personal Information compromised in the Data Breach.

145. Defendants had a special relationship with Plaintiffs and Class Members. The willingness to share and entrust Plaintiffs' and Class Members' Personal Information with Defendants was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Personal Information stored therein) and to implement security practices to protect the Personal Information they collected and stored.

146. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Personal Information.

147. Defendants also had independent duties under state law requiring them to reasonably safeguard Plaintiffs' and Class Members' Personal Information and promptly notify them about the Data Breach. Defendants breached those duties through the conduct previously alleged herein.

148. But for Defendants' wrongful and grossly negligent breach of the duties they owed Plaintiffs and Class Members, Plaintiffs' and Class Members' Personal Information either would not have been compromised or they would have been able to prevent some or all of their damages.

149. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of certainly impending future harm.

150. The injury and harm Plaintiffs and Class Members suffered, as alleged above, was and is reasonably foreseeable.

151. The injury and harm Plaintiffs and Class Members suffered, as alleged above, was the direct and proximate result of Defendants' negligent conduct.

152. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract

153. Plaintiffs incorporate herein every previously alleged factual allegation.

154. Plaintiffs bring this count on behalf of the National Class or, in the alternative, the Pennsylvania Subclass, Tennessee Subclass, and/or Georgia Subclass.

155. When Plaintiffs and Class Members provided their Personal Information to Defendants in exchange for Defendants' products, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their Personal Information.

156. Defendants solicited and invited Plaintiffs and Class Members to provide their Personal Information as part of Defendants' regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts

between Plaintiffs and Class Members on one hand, and Defendants on the other hand. Plaintiffs and Class Members accepted Defendants' offers by providing their Personal Information to Defendants in connection with purchases on Defendants' websites.

157. When entering into these implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

158. Defendants' implied promise to safeguard Plaintiffs' and Class Members' Personal Information is evidenced by a duty to protect and safeguard Personal Information that Defendants required Plaintiffs and Class Members to provide as a condition of entering into credit and debit card transactions with Defendants.

159. Plaintiffs and Class Members paid money to Defendants to purchase items at Defendants' websites. Plaintiffs and Class Members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

160. Plaintiffs and Class Members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from customers' continued use of Defendants' card payments system to make purchases—that Defendants would adequately safeguard Personal Information. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Class Members.

161. Plaintiffs and Class Members value data security and would not have provided their Personal Information to Defendants in the absence of Defendants' implied promise to keep the Personal Information reasonably secure.

162. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

163. Defendants breached their implied contracts with Plaintiffs and Class Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

164. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and Class Members sustained damages as alleged herein.

165. Plaintiffs and Class Members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

166. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 201-1, *et seq.*

167. Plaintiff Rossi incorporates herein every previously alleged factual allegation.

168. Plaintiff Rossi brings this count on behalf of the Pennsylvania Subclass.

169. Plaintiff Rossi, Pennsylvania Subclass Members, and Defendants are "persons" as defined by 73 Pa. Stat. § 201-2(2).

170. Plaintiff Rossi and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce" as defined by 73 Pa. Stat. § 201-2(3).

171. Plaintiff Rossi and Pennsylvania Subclass Members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

172. Defendants engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined by 73 Pa. Stat. § 201-2(4) by, among other things, engaging in the following conduct:

a. Representing that their goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that their goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that their goods and services were of a particular standard or quality when they were of another standard or quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix)); and

d. "Engaging in any other . . . deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

173. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

174. Defendants' unfair or deceptive acts and practices include but are not limited to:

a. failing to implement and maintain reasonable data security measures to protect Personal Information;

b. failing to identify foreseeable data security risks and remediate the identified risks;

c. failing to comply with common law duties, industry standards, and FTC guidance regarding data security; and

d. omitting and concealing the material fact that it did not have reasonable measures in place to safeguard such Personal Information.

175. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security practices and ability to protect customers' Personal Information.

176. Defendants intended to mislead consumers and induce them to rely on their misrepresentations and omissions, and Plaintiff Rossi and Pennsylvania Subclass Members did rely on Defendants' misrepresentations and omissions relating to their data privacy and security.

177. Plaintiff Rossi and Pennsylvania Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

178. Had Defendants disclosed to consumers that their data security systems were not secure and, thus, were vulnerable to attack, Plaintiff Rossi and Pennsylvania Subclass Members would not have given their Personal Information to Defendants.

179. Defendants acted intentionally, knowingly, and maliciously in violating 73 Pa. Stat. § 201-1, *et seq.*, and recklessly disregarded consumers' rights.

180. As a direct and proximate result of Defendants violation of violating 73 Pa. Stat. § 201-1, *et seq.*, Plaintiff Rossi and Pennsylvania Subclass Members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as alleged herein.

181. Plaintiff Rossi and Pennsylvania Subclass Members seek all remedies available under 73 Pa. Stat. § 201-1, *et seq.*, including, but not limited to, the damages expressly permitted under 73 Pa. Stat. § 201-9.2: actual damages or statutory damages of $100, whichever is greater;

treble damages defined as three time the actual damages; reasonable attorneys' fees and litigation costs; and any other such additional relief the Court deems necessary or proper.

182. Plaintiff Rossi and Pennsylvania Subclass Members also seek injunctive relief as set forth herein.

COUNT IV
Violations of the Tennessee Personal Consumer Information Release Act, Tenn. Code. Ann § 47-18-2107, *et seq.*

183. Plaintiff Parker incorporates herein every previously alleged factual allegation.

184. Plaintiff Parker brings this count on behalf of the Tennessee Subclass.

185. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

186. Plaintiff Parker and Tennessee Subclass Members' Personal Information that was compromised in the Data Breach includes Personal Information as covered under Tenn. Code Ann. § 47-18-2107(a)(3)(A).

187. Defendants are required to accurately notify Plaintiff Parker and Tennessee Subclass Members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Parker's and Tennessee Subclass Members' Personal Information in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

188. Because Defendants discovered a breach of their security systems in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Defendants have an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

189. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

190. As a direct and proximate result of Defendants' violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff Parker and Tennessee Subclass Members suffered damages, as described above.

191. Plaintiff Parker and Tennessee Subclass Members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f) including actual damages and injunctive relief.

COUNT V
Violations of the Tennessee Consumer Protection Act, Tenn. Code. Ann § 47-18-101, *et seq.*

192. Plaintiff Parker incorporates herein every previously alleged factual allegation.

193. Plaintiff Parker bring this count on behalf of the Tennessee Subclass.

194. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity, or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

195. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…"

196. Defendants' online sales of jewelry and accessories constitute "trade or commerce."

197. Defendants' conduct violates the Tennessee Consumer Protection Act because Defendants engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff Parker's and the Tennessee Subclass's Personal Information in spite of assurances to the contrary.

198. Defendants omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff Parker and Tennessee Subclass Members' Personal Information, which were deceptive, false and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which Defendants knew, or by the exercise of reasonable care, should have known, to be untrue, deceptive or misleading. Such conduct is unfair, deceptive, untrue, or misleading in that Defendants: (a) represented that their services have approval, characteristics, uses or benefits that they do not have; and (b) represented that services are of a particular standard, quality or grade.

199. Defendants' materially misleading statements and deceptive acts and practices alleged herein were directed at the public at large.

200. Defendants' actions impact the public interest because Plaintiff Parker and the Tennessee Subclass have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendants' generalized course of deception as described throughout this Complaint.

201. Defendants' acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

202. Defendants' misrepresentations, misleading statements and omissions were materially misleading to Plaintiff Parker and members of the Tennessee Subclass.

203. Defendants' violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendants, among other things, knew that their policies and procedures for the protection of Plaintiff Parker's and the Tennessee Subclass' Personal Information were inadequate to protect that Personal Information. Nonetheless, Defendants continued to solicit and process Personal Information in the United States in order to increase their own profits.

204. Had Plaintiff Parker and the members of the Tennessee Subclass known of Defendants' misrepresentations, misleading statements and omissions about their use of Personal Information, they would not have made online purchases at Defendants' website.

205. As a direct and proximate result of Defendants' conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff Parker and the members of the Tennessee Subclass have been injured in amounts to be proven at trial.

206. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff Parker and the Tennessee Subclass are entitled to make claims against Defendants for ascertainable damages in an amount to be determined at trial. Plaintiff Parker also properly asks that such damages be trebled based on Defendants' knowledge and/or intention with respect to their breach.

207. Plaintiff Parker also seek injunctive relief, including a robust, state of the art notice program for the wide dissemination of a factually accurate statement on the actual state of Defendants' Personal Information storage and the implementation of a corrective advertising campaign by Defendants.

208. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff Parker and the Tennessee Subclass make claims for attorneys' fees and costs.

COUNT VI
Violations of the Georgia Security Breach Notification Act, O.C.G.A. § 10-1-912, *et seq.*

209. Plaintiff Holmes incorporates herein every previously alleged factual allegation.

210. Plaintiff Holmes brings this count on behalf of the Georgia Subclass.

211. Defendants are businesses that own or license computerized data that includes Personal Information as defined by O.C.G.A. § 10-1-912(a).

212. Plaintiff Holmes and Georgia Subclass Members' Personal Information that was compromised in the Data Breach includes Personal Information as covered under O.C.G.A. § 10-1-912(a).

213. Defendants are required to accurately notify Plaintiff Holmes and Georgia Subclass Members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Holmes's and Georgia Subclass Members' Personal Information in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

214. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated O.C.G.A. § 10-1-912(a).

215. As a direct and proximate result of Defendants' violations of O.C.G.A. § 10-1-912(a), Plaintiff Holmes and Georgia Subclass Members suffered damages, as described above.

216. Plaintiff Holmes and Georgia Subclass Members seek relief under O.C.G.A. § 10-1-912, including actual damages and injunctive relief.

COUNT VII
Unjust Enrichment

217. Plaintiffs incorporate herein every previously alleged factual allegation.

218. Plaintiffs bring this count in the alternative to Plaintiffs' breach of implied contract count.

219. Plaintiffs bring this count on behalf of the National Class or, in the alternative, the Pennsylvania Subclass, Tennessee Subclass, and/or Georgia Subclass.

220. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Defendants received and retained money belonging to Plaintiffs and Class Members directly through purchases made on Defendants' websites.

221. Defendants had knowledge of the benefits conferred on them by Plaintiffs and Class Members.

222. The money that Plaintiffs and Class Members paid directly to Defendants was supposed to be used by Defendants, in part, to pay for the costs of reasonable data privacy and security practices and procedures for the collection, storage, and use of Plaintiffs' and Class Members' Personal Information.

223. As a result of Defendants' conduct, Plaintiffs and Class Members suffered damages in an amount equal to the difference in value between the online transactions with the reasonable data privacy and security practices and procedures for which they paid, and the transactions without reasonable data privacy and security practices and procedures that they actually received.

224. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement (or to adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members reasonably expected and paid for and that were otherwise mandated by state law and industry standards.

225. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendants received.

226. The Court should impose a constructive trust on all unlawful or inequitable sums Defendants received traceable to Plaintiffs and Class Members.

COUNT VIII
Declaratory Judgment

227. Plaintiffs incorporate herein every previously alleged factual allegation.

228. Plaintiffs bring this count on behalf of the National Class or, in the alternative, the Pennsylvania Subclass, Tennessee Subclass, and/or Georgia Subclass.

229. Defendants owe duties of care to Plaintiffs and Class Members, which require them to adequately secure Personal Information.

230. Defendants still possess Personal Information regarding Plaintiffs and Class Members.

231. Although Defendants claim they have "reinforced the security of our site," they have provided no detail on what, if any, fixes they have actually made.

232. Plaintiffs and Class Members are at risk of harm due to the exposure of their Personal Information and Defendants' failure to address the security failings that lead to such exposure.

233. There is no reason to believe that Defendants' security measures are any more adequate than they were before the breach to meet Defendants' contractual obligations and legal duties, and there is no reason to think Defendants have no other security vulnerabilities that have not yet been exploited.

234. Plaintiffs, therefore, seek a declaration that: (1) Defendants' existing security measures do not comply with their implicit contractual obligations and duties of care to provide

reasonable security procedures and practices appropriate to the nature of the information to protect customers' Personal Information; and (2) to comply with their implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing lifetime credit monitoring services for Plaintiffs and Class Members; and

h. Meaningfully educating its users about the threats they face as a result of the loss of their Personal Information to third parties, as well as the steps Defendants' customers must take to protect themselves.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, respectfully request the Court order relief and enter judgment in their favor and against Defendants as follows:

A. An order certifying this action as a class action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein.

B. Plaintiffs request injunctive and other equitable relief as is necessary to protect the interests of the Class, including:

i. an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein; and

ii. requiring Defendants to protect all data collected or received through the course of their business in accordance with applicable law and best practices under industry standards;

iii. requiring Defendants to design, maintain, and test their computer systems to ensure that Personal Information in their possession is adequately secured and protected;

iv. requiring Defendants to disclose any future data breaches in a timely and accurate manner;

v. requiring Defendants to engage third-party security auditors as well as internal security personnel to conduct testing, including simulated attacks,

penetration tests, and audits on Defendants' systems on a periodic basis and ordering them to promptly correct any problems or issues detected by these auditors;

vi. requiring Defendants to audit, test, and train their security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner;

vii. requiring Defendants to implement multi-factor authentication;

viii. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices;

ix. requiring Defendants to encrypt all Personal Information;

x. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

xi. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

xii. requiring Defendants to purge, delete, and destroy in a reasonably secure and timely manner Personal Information no longer necessary for their provision of services;

xiii. requiring Defendants to conduct regular database scanning and security checks;

xiv. requiring Defendants to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xv. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class Members; and

xvi. requiring Defendants to educate all Class Members about the threats they face as a result of the loss of their Personal Information to third parties, as well as steps Class Members must take to protect themselves.

C. A judgment awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, punitive damages, treble damages, statutory damages, exemplary damages, equitable relief, restitution, and disgorgement;

D. An order that Defendants pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

E. Pre-judgment and post-judgment interest;

F. Attorneys' fees, expenses, and the costs of this action; and

G. All other and further relief as this Court deems necessary, just, and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully submitted,

Dated: October 26, 2020

/s/ Bradley K. King

Tina Wolfson
twolfson@ahdootwolfson.com
Bradley K. King
bking@ahdootwolfson.com
Theodore W. Maya
tmaya@ahdootwolfson.com
Henry Kelston

hkelston@ahdootwolfson.com
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585

M. Anderson Berry
aberry@justice4you.com
Leslie Guillon
lguillon@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, California 95825
Tel: (916) 777-7777
Fax: (916) 924-1829

Katrina Carroll
kcarroll@carlsonlynch.com
Kyle A. Shamberg
kshamberg@carlsonlynch.com
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
Tel: (312) 750-1265

Rachele R. Byrd
byrd@whafh.com
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Tel: (619) 239-4599
Fax: (619) 234-4599

Carl V. Malmstrom
malmstrom@whafh.com
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLC
111 W. Jackson Blvd.,
Suite 1700 Chicago, Illinois 60604
Tel: 312/984-0000
Fax: 212/545-4653

Counsel for Plaintiffs and the Proposed Class

EXHIBIT 1

claire's | ICING

July 7, 2020

109 1 24344 **********AUTO**ALL FOR AADC 370
DELILAH PARKER
[redacted]

Dear Delilah Parker,

Claire's and Icing are writing to let you know that we recently identified and addressed an incident that may have involved your payment card information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?

We recently began an investigation of our e-commerce websites, and on June 12, 2020 we identified and removed computer code that had been added to our site by an unauthorized person. The added code was capable of obtaining information entered by customers during the checkout process and sending that information out of our system. A security firm was engaged and we identified the specific transactions involved. We also reinforced the security of our site. Purchases made in our retail store locations were not involved.

Findings from the investigation show the code was first added on April 7, 2020. There were several times from April 7 to June 12 when the added code was not present because of new code deployments. We are notifying you because you placed an order during a time the added code was present.

What Information Was Involved?

The information entered during the checkout process that could have been copied includes:

- **Contact information** - first and last name, address, email address (only if you chose to edit your email on the checkout page), and phone number.
- **Payment card information** - payment card number, expiration date, and card verification code for the payment card ending in 7707. If you made more than one purchase between April 7 and June 12 and used more than one card, you can identify the other cards involved by looking at your email receipt or by calling us at the number below.
- **Other information** - if you paid with a gift card or created a Claire's account during the checkout process, the added code could have copied the gift card number and PIN or the account password (but not email address).

What We Are Doing.

Claire's conducted an investigation, implemented additional security measures, and hired resources to inform and assist our customers. We also notified the payment cards network so that they can inform the banks that issued the cards. Claire's also notified law enforcement and relevant authorities.

We are also offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with internet surveillance and identity theft insurance at no cost to you upon enrollment. To activate your membership and start monitoring your personal information please follow the steps on page 3.

What You Can Do.

We encourage you to closely review your payment card account statements for any unauthorized charges. You should immediately report any unauthorized charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported.

CERTIFICATE OF SERVICE

I hereby certify that on October 26, 2020, the foregoing Consolidated Amended Class Action Complaint was electronically filed with the Clerk of the United States District Court for the Northern District of Illinois, using the CM/ECF system, which will send notification of the filing to all attorneys of record.

/s/ Bradley K. King